Russian Views on Information-based Warfare

by Timothy L. Thomas
Foreign Military Studies Office, Fort Leavenworth, KS.
July 1996

This Article Appeared in the 1996 Special Edition of
Airpower Journal

"From a military point of view, the use of information warfare means against Russia or its armed forces will categorically not be considered a non-military phase of a conflict, whether there were casualties or not...considering the possible catastrophic consequences of the use of strategic information warfare means by an enemy, whether on economic or state command and control systems, or on the combat potential of the armed forces,...Russia retains the right to use nuclear weapons first against the means and forces of information warfare, and then against the aggressor state itself."[1]

INTRODUCTION

In the former Soviet Union, wide-spread integration of computer technology was delayed by two factors: the Soviet's iron grip over most information and technology systems (xerox machines, personal computers, patents, etc.); and a reluctance to study information systems seriously. In fact, the West had an early unchallenged entry into the computer age, since cybernetics was officially proscribed by General Secretary Nikita Khrushchev only during the late 1950s. Today, however, Russian interest in information systems is intense and new users come on-line daily. Unfortunately, laws governing the control, use and sale of this technology lack enforcement. Russian software and hardware piracy are widespread. As a result, computers will proliferate quickly throughout Russia during the next few years. The availability of pirated technology will allow Russia to quickly catch and perhaps surpass even our own technologicalcompetency in some areas. In the information age, there is little room for complacency.

This article attempts to define the Russian understanding of the term information warfare, and explores the impact of the information revolution on the Russian military. Like the U.S., the Russian Army is still discussing terminology, concepts, and policy, and has no authoritative definitions or doctrine to offer the international community. In fact, until it catches up with the West in the information technology arena, Russia may be content to use the nuclear deterrent to offset the possibility of anyone using an information operation against them, as the introductory quote to this section demonstrates. Such an option is dangerous for everyone.

Russia, the U.S., and other nations with the information weapon need to begin joint discussions on specific aspects of information warfare now. Otherwise, we will enter yet another weapons race, this one over how to attack information systems through the electromagnetic spectrum (via third generation nuclear weapons) or to destroy software (via sophisticated computer viruses).[2] At the same time, cooperation is mandated to keep priceless technology out of the hands of criminals or terrorists.

This article has one caveat. The Russian military officers who have openly addressed the subject of the military's information revolution do not officially represent the Russian Ministry of Defense (MOD) or General Staff. Therefore this study avoids the phrase "the Russian military thinks" since it cites individual military or civilian analysts.

DEFINING INFORMATION WARFARE

While no official (that is, MOD endorsed) military definition of information warfare was found in the research for this article, several unofficial ones were uncovered.[3] The most authoritative were two provided by Russian officers at the General Staff Academy, one defining information war (they used the Russian "informatsionnoye protivoborstbo" or information confrontation) in a technical/psychological manner:

Information warfare is a way of resolving a conflict between opposing sides. The goal is for one side to gain and hold an information advantage over the other. This is achieved by exerting a specific information/psychological and information/technical influence on a nation's decision-making system, on the nation's populous and on its information resource structures, as well as by defeating the enemy's control system and his information resource structures with the help of additional means, such as nuclear assets, weapons and electronic assets.[4]

The operational-strategic version defined information war as follows:

Within the framework of the execution of the operational-strategic (operational) missions of offensive and defensive troop units, information warfare consists of the specially planned and coordinated-integrated actions of the forces and assets of intelligence and early warning, command and control, communications, deception and electronic warfare, whose purpose is to guarantee the achievement of the goals of the operation (of its combat actions).[5]

A Ministry of Defense civilian analyst offered yet another definition of information war (he preferred the Russian "informatsionnoya voyna" or information war), noting that:

"Both a broad and narrow sense are inherent in the existing concept of information warfare. In the broad sense, information warfare is one of the varieties of the "cold war"- countermeasures between two states implemented mainly in peacetime with respect not only and not so much to the armed forces as much as to the civilian population and the people's public/social awareness, to state administrative systems, production control systems, scientific control, cultural control, and so forth. It is namely in this sense that the information security of the individual, society, and state is usually understood . . . In the narrow sense, information warfare is one of the varieties of military activity/operations/actions (or the immediate preparation for them) and has as its goal

the achievement of overwhelming superiority over the enemy in the form of efficiency, completeness, and reliability of information upon its receipt, treatment, and use, and the working out of effective administrative decisions and their purposeful implementation so as to achieve combat superiority (victory) on the basis of this. The waging of information warfare in the narrow sense is the field of responsibility of mainly the ministers of defense of modern states."[6]

Despite the absence of an official MOD blessed definition for information warfare, these definitions suffice to give us a good general overview of how the Russians are thinking about information warfare. However, based on published materials in the military and open press, other key components of the Russian understanding of the term are identifiable. These components offer an understanding of information warfare far beyond those cited above, and include the following topics: - the role of the Federal Agency for Government Communications and Information (FAPSI) in combating "information weapons"; - the use of computer (combat) viruses as a means of warfare; - the importance of the information component in the calculation of combat potential; - the necessity to build information collection, processing, and utilization systems (reconnaissance and intelligence systems) and systems that deny information (electronic warfare and counterintelligence systems) both in peacetime and on the field of battle; - the special work of "information manipulation, perception management, and reflexive control" performed by the mass media and elements of special designation (such as psychological operations [PSYOP] elements).

Each of these elements are discussed below in more detail.

The civilian (FAPSI) view of information security.

"An exchange of information strikes (ydarov) is becoming extremely dangerous for the fate of the world, since the effectiveness of these strikes are rapidly growing, and it is becoming increasingly difficult to determine their sources."[7]

Threats in the area of information security are increasing. Nine-tenths of all information, according to one Russian source, now circulates in radio electronic form. This aids unauthorized access. In addition, in a world becoming increasingly computerized, there have emerged new, socially dangerous crimes and harmful effects from the use of information technology.[8]

The agency charged with information security in Russia since 19 February 1993 is the Federal Agency for Government Communications and Information, or FAPSI. As one writer noted:

"The law assigns four matters to FAPSI's jurisdiction: special communications (including government communications), the cryptographic and engineering-technical security of encrypted communications, intelligence gathering activities in the sphere of special communications, and the provision of special information to higher bodies of authority."[9]

FAPSI appears to fulfill many of the missions of the U.S. National Security Agency. It also fights against domestic criminals and hackers, foreign special services, and "information weapons" that are for:

" . . . gaining unsanctioned access to information and putting electronic management systems out of commission, and for enhancing the information security of one's own management systems. The potential damage from the use of "information weapons" against government information and telecommunications systems, systems for the command and control of strategic missile forces, and systems for the management of transportation, power engineering and credit and financial structures can be compared to the effects of weapons of mass destruction, since they can be used, in principle, to destroy the entire system of state administration."[10]

Russia considers information weapons extremely dangerous, and views information and telecommunications technologies as independent from one another. To combat this fact, FAPSI has developed for state administrative agencies a protected, special-purpose Federal Information and Telecommunications System (SFITS).[11] Russia, with this system, considers itself the "only country which is capable of providing 100% security for consumers at the very first stage of the mass introduction of SFITS in daily life. The contribution which FAPSI can make to our overall security cannot be overestimated."[12] The head of FAPSI, Aleksandr Starovoytov, is less optimistic. In a July 1995 interview, he noted that foreign special services are using the "information weapon" as one of the main areas of their activity, and that several government agencies in Russia are vulnerable to electronic surveillance devices.[13] Russia also has created an Academy of Cryptography, which it believes is the only one in the world.[14]

FAPSI officials are paying special attention to information security in the credit, financial, and banking circles as well. The state has instituted licensing and certification to ensure that organizations can safeguard the state, commercial, and personnel secrets of any nation. To date only 53 of 250 firms operating in the information security field have applied under Russian Federation edict No 334. Law enforcement agencies are charged with stopping activities of firms that are violators.[15]

The military, in turn, has also recognized the need for a security system, especially for military software and command and control systems. As late as 1994, the military continued to view its information security policy as "porous as Swiss cheese" to a variety of threats. A military officer, writing in the journal *Voennaya Mysl* (*Military Thought*), noted that the sources of destabilizing factors causing information threats included individuals, organizations, associations, hostile states, coalitions, and the environment. Even up-to-date information systems, he added, can quickly change from a stabilizing to a destabilizing factor, since they can activate information threats, implant these threats in individual minds or the public consciousness, or serve as a generator of spontaneous threats emerging from technical failures.[16]

Computer virus warfare

"After the surfacing of hostilities, combat viruses and other information-related weapons can be used as powerful force multipliers by their synergistic or mutually deprecating effects from multiple weapon types in proximity to one another."[17]

The Russian military is studying **virus or software warfare** as one of the most important aspects of future information warfare. Virus warfare presents special problems at the strategic level because "its use bears an impersonal imprint, is easily disguised either as banal computer

hooliganism, or, on the contrary, can openly portray itself as measures to protect copyright and commercial rights of firms for their own software."[18] In fact, as the willingness to use traditional means of warfare diminish, there may not exist a reason to decide matters through violence, especially if virus warfare is successful. As one Russian officer noted:

"There is no need to declare war against one's enemies and to actually unleash more or less large military operations using traditional means of armed struggle. This makes plans for "hidden war" considerably more workable and erodes the boundaries of organized violence, which is becoming more acceptable."[19]

The use of virus or software/hardware warfare in specific instances, and the computerization/miniaturization of weaponry to ensure accuracy, underscore the fact that the Russian army believes it is passing from a **correlation of forces based on probability to one based on precision kills or virus implants.**

Viruses are viewed as force multipliers that can turn the initial period of war into pure chaos if they are released in a timely manner. In the opinion of one officer, there are several viruses with which to contend. They are the Trojan horse virus (remains idle for a certain period of time and then causes catastrophic destruction of the system); the forced quarantine virus (knocks out the program of the unit into which it was planted, and it will destroy the entire system if its components are not separated); the overload virus (quickly spreads throughout the entire system and gradually slows its operation); and the sensor virus (penetrates a preplanned sector of a computer's data-storage area and destroys the data bank and its information at a critical moment).[20]

One Russian officer accused the U.S. of establishing a special service known as Computer Virus Countermeasures to engage in the introduction of bugs into the software of likely enemies. This makes war plans more realistic, he asserted, and erases the line establishing the initial period of war, since these actions are begun in peacetime. It also adds another dimension to the principle of surprise.[21]

The problem of computer viruses became particularly acute for Russian software security specialists when the USSR ceased to be one gigantic "information space" and the republics broke away as independent entities. All weapons or command posts shared similar if not identical software programs. After the breakup, the possibility of a virus attacking all such systems increased.

"The altered composition of the Union casts doubt upon the existence of a single strategic military territory and consequently, a single information space, which can lead to the employment of "information weapons" directly through the information nets within the nation's territory."[22]

The Russian military is working hard to overcome this shortcoming, as well as to establish new parameters for safeguarding the countries information space and for detecting and destroying viruses, a most difficult task. It has created antiviruses which in turn have spawned the appearance of diversionary programs, the most sophisticated of which the Russians call "stealth

viruses." This virus does not act in the normal manner, that is, it does not expose itself in the form of an enlarged file. Instead, the stealth virus conceals itself within a file while the file retains its original size and shape. The Russian military has developed a complicated mathematical procedure that compares the files on a disk with file structures and virtual free space to uncover a stealth virus.[23]

The information component of combat potential

The Gulf War demonstrated to the Russians the changing ratio among attack, tacticalcommand and control, and information support systems in the accomplishment of combat missions. Some Russian officers assessed victory as coming from overwhelming superiority in logistics and in combat and information support systems (the command, control, communications, and intelligence [C3I] system).

[24] Another fundamental distinction was the fact that, for the first time, the side with the preponderance of weaponry did not win. The combat potential of forces manifested themselves in a new way. As one Russian military theorist noted:

"It's time to recognize the need to relook fundamental priorities in the very structure of the armed forces, in the correlation of branches and combat arms, in their technical armament, and in questions of command and control, combat support and personnel training, placing emphasis on the qualitative parameters of military organizational development...it appears possible to conclude that **in analyzing the sides' combat potential in operations it is necessary to place paramount importance on technological indicators of new weapons,** which are capable of largely predetermining the end result of military operations."[25]

The current scientific advisor to Russia's national security council, retired Admiral V.S. Pirumov, supported this view in another 1992 *Military Thought* article. Information support, in his view, predetermined the development of a new generation of reconnaissance equipment that led to more precise target location. Computer-aided troop and weapons control stations were also made possible by applying information support technology. End users as low as battalion staffs or the individual soldier in the field can use this technology. Pirumov estimated that the use of information technology increased the combat capability of the multinational force by a factor of two.[26] Regarding the Persian Gulf conflict he added:

"All this makes possible the conclusion that the priority and weight of the contribution of information support to troop combat effectiveness in developed countries determined the dominant role of the "electronic/fire" concept of conducting warfare."[27]

If two force groupings have equal combat potentials in weapons, but one has an advantage over the other in information means, the combat potential of that side will be much higher. This is an exact science in the Russian army.[28] Again, Pirumov notes:

"There are developed methodologies (including machine methodologies) to calculate values of specific indicators of each kind of weapon, units, formations and large strategic formations of forces permitting an assessment of the contribution of all information support equipment with

consideration of its correlation, character and content, and the operational-tactical conditions of accomplishing assigned combat missions."[29]

Pirumov adds that the ratio of combat potential between forces can find use in estimating both military-strategic parity between states and operational-strategic parity between opposing formations. If formerly the combat potential ratio reflected the qualitative and quantitative comparison between the sides' forces and weapons systems, now the ratio is meaningless without calculating the information component of the combat potential of a force grouping.[30] Armed struggles of the modern era involve a struggle for superiority in information over the opposing side, evolving as one of the indispensable factors in ensuring victory over an enemy. Retired Russian General Panov believes that two areas need further development. The first is the development of non-lethal, impact weapons for troops currently employed in peace operations. These are lifesaving weapons that are humanitarian due to their physical and chemical composition. The second area of development is that of "functional destruction means" weaponry, the electromagnetic, high-frequency pulse weapons which can serve as a deterrent for high-precision weapons.[31] The latter use is particularly significant in that it can negate the effectiveness of weapons based on information technology. Russian interest in electromagnetic pulse weapons is not new. Retired Russian General Belous, a nuclear weapons specialist, believes that enhanced "super" electromagnetic pulse (EMP) weapons, nuclear shrapnel for use in space, penetrating warheads that destroy C3I assets, and X-ray lasers all belong to fourth generation nuclear weaponry. He added:

"Fifth generation nuclear weapons, those based on new physical principles, include those which will act on the human organism to bring about disruption of its physical or mental capacities. Belous also discussed sixth generation or "fundamentally new types of weapons" to include: geophysical, electro-magnetic or radio frequency, infrasonic, genetic, ethnic, psychotronic, beam, laser, and non-lethal weapons. There could be fundamental breakthroughs in the natural sciences which could make possible other types of weapons we cannot even anticipate at this time."[32]

Information accumulation, processing, adaptation, and integration

In 1993 Russian V.N. Medvedev defined the dissemination of information technology in the armed forces as "the process of the creation, broad-scale incorporation and application in various fields of activity of the armed forces, under any conditions, of methods, systems and means of obtaining, gathering, processing, storing and using information."[33] To the Russians, this process is the key to informed decision-making. A certain amount of information about the other side's forces is required. Fast reacting processors are mandatory since an increase in the existing volume of information lengthens the time required for organizing and preparing for combat, and the probability of information aging grows in accordance with an increase in the volume of information.[34] Therefore the timely gathering and utilization of information is of extreme importance.

After the Gulf War, the Russians wrote that they considered the development of superiority in data collection, processing and representative information **as a new phenomenon of the conflict**. In the past, opposing sides tried to gain numerical superiority in the types of weapons

and pieces of military equipment.[35] Information accumulation, processing and adaptation are now just as important, especially in reconnaissance and electronic warfare systems.

At the same time, Russia expects to direct considerable effort toward disrupting the enemy's information support system. The goal is to forestall his ability to collect, gather, transmit and process information. Another mission is "to disinform the enemy in every way, while safeguarding possible channels of a leak of especially important information."[36]

The integration of information obtained from reconnaissance and electronic countermeasures (ECM) equipment, and command and control equipment is a critical component of what the Russian military terms *combat systems theory*. The goal is to integrate information quickly into systems requiring constant data links for accurate responses. The concept allows combat systems to create a synergy of effort that exceeds the sum of the combat potentials of individual systems.

Information manipulation/perception management

Disinformation is a Russian technique that manipulates information and misinforms people or groups. Some disinformation procedures are obvious, some unconvincing, and some work through delayed perceptions, rumors, repetition, or arguments. Specific persons or particular social groups can serve as disinformation targets. The purpose of a disinformation campaign is to influence the consciousness and mind of man. In Russia today, where there is an unstable public-political and socio-economic situation, the entire population could serve as the target of influence for an enemy campaign.

[37] The authorities in Moscow recognize this and are trying to gain control over a most dangerous situation in their view. Clearly, the management of information is essential to their maintenance of stability.

Historically, the Soviet Union was very good at developing theories of information management. Their propaganda machine stood at the apex of this effort. One of their most interesting Cold-war methods for managing information and getting people (or an opponent) to do what an action's initiator wanted was described by the theory of **reflexive control**. Reflexive control is a "branch of the theory of control related to influencing the decisions of others. In a military context, it can be viewed as a means for providing one military commander with the ability to indirectly maintain control over his opponent commander's decision process."[38] Reflexive control involves creating a pattern or providing partial information that causes an enemy to react in a predetermined fashion without the enemy realizing that he is being manipulated. Its aim is to force an enemy commander to make a decision that, through the manipulation of information, was predetermined by the opposing side.

Vladimir Lefebvre, a Soviet researcher assigned to the First Computer Center of the Soviet Ministry of Defense (also known as Military Unit 01168) and one of the best Soviet minds working on the project of influencing an enemy's actions, worked on reflexive control in the late 1950s and early 1960s. His opinion is that:

" . . . in making his decision the adversary uses information about the area of conflict, about his own troops and ours, about their ability to fight, etc. We can influence his channels of information and send messages which shift the flow of information in a way favorable for us. The adversary uses the most contemporary method of optimization and finds the optimal decision. However, it will not be a true optimum, but a decision predetermined by us. In order to make our own effective decision, we should know how to deduce the adversary's decision based on information he believes is true. The unit modeling the adversary serves the purpose of simulating his decisions under different conditions and choosing the most effective informational influence."[39]

A review of the modern Russian military press indicates that this theory is still in force. For example, in a July 1995 issue of the journal *Morskoy Sbornik* Major General (retired) M. Ionov wrote an article on "Control of the Enemy." It requires "the art of choosing special methods of bringing pressure to bear on him, consideration of many factors, the ability to determine the place and time to apply different combinations of such pressure, the ability to evaluate phenomena and forecast their development, and the presence of high intellect, great professional knowledge and strong will", as well as the use of nonrepetitive techniques and combinations for the proper physical and psychological effect on the enemy. To control the enemy and simultaneously stop his efforts of countercontrol, information is needed on the status of enemy forces, on the nature of their actions, and on their capabilities.[40]

Ionov offered several principles for "control of the enemy." First, he noted the reflexive nature of the response desired; that is the commander must picture for himself a possible enemy response to the conditions he desires to impose. A second feature is the probabilistic nature of the response, since the enemy may uncover the activity and institute his own countercontrol measures. A third principle to note is the growing importance of the level of development of technical combat assets, especially reconnaissance (this also makes the exposure of an action aimed at disinforming the enemy more likely). A final principle is the use of harsh forms of pressure on the enemy, those that take into account social elements and intellectual, psychological, ethical and ideological factors. Examples would be the deliberate cruelty toward the civilian population or prisoners of war of a conflict region, a declaration of unrestricted submarine warfare (to include the sinking of any vessels to include those of neutral countries), and so on.[41]

A recent article on information warfare by three Russian civilians noted that the Russians considered the Strategic Defense Initiative (SDI) of the U.S. during the Cold War as a reflexive control mechanism designed to financially exhaust the Soviet Union. Now, the authors add, the U.S. may be trying to do the same to Russia through its emphasis on information warfare.[42]

CONCLUSION

This article has presented a general outline of the Russian view of information warfare through the writings of various military and civilian figures. There is a degree of urgency for the Russian army to modernize its force and take the study of information warfare and associated topics from the theoretical to the practical level. There are many problems to crack. In one article that

appeared over two years ago, the following were listed as priority problems for the Russian armed forces in the information area:

- creating a telecommunications environment and its lash-up with nation-wide communications and data-transmission systems;

- developing and incorporating base problem-oriented systems;

- equipping the armed forces staffs and organizations quickly with the basics of information technology and personal computers, advanced communications and telecommunications gear, and improved organizational techniques to adopt a "paperless" information technology;

- improving tools and methods for developing software and the use of computer assisted technologies;

- assuring technical, information, linguistic, and program compatibility;

- improving the system of training, retraining, and skill enhancement of military specialists;

- and creating standardized, advanced means of information technology.[43]

Information technology acquisition represents a way to quickly catch up with the West, since much off-the-shelf technology is available. It is also one of the best ways to increase combat capabilities.

Apart from the military-technical component of information warfare, another requirement was identified: to control information about society and its armed forces in an environment permeated by unstable military-political and socio-economic conditions. The Russian military's perception of information warfare, as a result, will most certainly include both external and internal psychological and propaganda aspects as well as military-technical components.

The West should not ignore these developments and requirements in Russia. Instead, it should initiate discussions with the Russian military to calm their anxiety and demonstrate our willingness to cooperate in this area much as we did in the nuclear area during the Cold War. This will lessen tension on both sides over the information technology race, promote understanding and perhaps the production of joint doctrines or systems (and hopefully joint terminology), and prevent a new arms race, this time over information sensitive systems, from developing.

One of the easiest ways for the West to begin joint talks on information warfare with Russia is through the medium of a conference among academics or through an unofficial organization or club. In Russia, one example of such a group is the International Information Academy. It is composed of both civilian academicians and military officers. The Academy could serve as a forum for broader discussions with the West and already appears oriented this way, having several foreigners on its membership roll. By starting this discussion soon, Russia and the West can prevent a new arms race over information systems and technologies from gaining

momentum and spinning out of control. With the rate of progress in the realm of information technology, time really is of the essence.

Endnotes

1. Doctor V.I.Tsymbal, "Kontseptsiya 'Informatsionnoy voyny'", (Concept of Information Warfare), speech given at the Russian-U.S. conference on "Evolving post Cold War National Security Issues," Moscow 12-14 September, p 7.BACK

2. What many U.S. analysts have termed "information warfare" is, in the view of retired Russian Major General Vladimir Slipchenko, simply a component of "Sixth Generation Warfare." He defined the first through the fifth generations of warfare as: wars during the time of slave-holding and feudal societies; the expansion of technological production and the appearance of gunpowder and smoothbore firearms; tube artillery and rifled small arms; the introduction of automatic weapons, tanks and military aircraft; and the technological and scientific revolutions of the last 50 years or so which produced the first nuclear missiles. Slipchenko defined sixth generation warfare as an impending development whose outline already includes as its centerpiece superior data-processing to support precision smart weaponry, command and control, reconnaissance, and electronic and air defense equipment. Vladimir I. Slipchenko, "A Russian Analysis of Warfare Leading to the Sixth Generation," *Field Artillery*, October 1993, pp 38-41. Slipchenko also noted that "today, the main threat to the security of a considerable number of countries is their backwardness in developing and rapidly accepting massive quantities of the latest precision weapons and data processing and electronic warfare equipment...Armed combat between enemies of different war generations will undoubtedly be won by the side armed with the latest smart weapons. Gone will be the need to maintain large troop formations and keep up a correlation of troops and material."BACK

3. In Russian, the "war" part of the term "information war" is translated as either informatsionniya "voyna," informatsionniya "borba," or informatsionnoye "protivoborstbo." According to one source, the term "informatsionniya voyna" is usually used in a wider sense by journalists rather than military professionals. The latter prefer the term "informatsionnoye protivoborstbo", which also means "information warfare" and is already in use by some military sources, to include the General Staff Academy. "Informatsionniya borba" is also used by military professionals, but how it is interpreted from the other two is unknown. It is still too difficult to say specifically which term will find preference. This is another reason to start discussions with the Russians, to find a common language not only for this term but for many others. Some examples follow.

In one 1994 article on information security, the term "informatsionniya borba" was used for information warfare, defining it as "including information support, information protection, and a number of information counter-measures aimed at blocking information of interest to various kinds of criminals and supplying them with false data." (See S.A. Komov, "O kontseptsii informatsionnoy bezopasnosti strany ("On the Concept of the Country's Information Security,") *Voyennaya Mysl* (*Military Thought*) No 4, 1994, pp 16-17). In this sense it had more of a defensive than offensive character, and applied equally to the internal Russian situation and to a

confrontation with a possible enemy beyond Russia's borders. It also possessed a disinformation aspect.

Colonel A. I. Pozdnyakov, a professor at the General Staff Academy, used two of the three terms cited above for information war, informatsionnoye protivoborstbo and informatisionniya borba, in addition to many supporting terms in one of his articles. Some of the terms encountered in Pozdnyakov's and other articles are listed at the annex on Terms and Definitions.BACK

4. Discussion with a Russian officer in Moscow, May 1995.

A recent bibliography offered by the same officer provides an example of an expanded understanding of information warfare. He subdivided information warfare (IW) into the following categories:

- philosophical problems of IW - information security as an aspect of national or global security - the information resource in the capabilities or potential of a government - the concept of IW - the informationalization of armed conflict

x electronic means of armed combat

x automatization of armed combat

x robotization of armed conflict

x intellectualization means of armed conflict (precision guided weapons)

- the informatization of combat (operational) preparations - the informatization of the field of battle (digitalization of the field of battle) - information-psychological warfare

x military-patriotic education of the population of the country

x the moral-psychological preparation of personnel of one's own armed forces

x psychological operations against the population and personnel of the armed forces of a country designated as a potential enemy

- informational-technological warfare

x the involvement of systems of control and communications in confrontation (C3)

x the role and place of intelligence in IW

x EW as a sphere of IW

x IW by means of special mathematical programs (software warfare)

x how to defeat information resources

x the redistribution of information resources

x the defense of information resources

- the preparation of personnel to take part in IW - the international law aspects of IWBACK

5. Ibid.BACK

6. Professor V.I. Tsymbal, "Kontseptsiya 'informatsionnoy voyny'" ("Concept of Information War"), paper received at conference with the Russian Academy of Civil Service in Moscow, 14 September 1995.BACK

7. A.I. Posdnyakov, "Informatsionnaya Bezopasnost'" ("Information Security"), *Bezopasnost'* (*Security*) (Russian publication of the International Security Foundation), No. 6, December 1992, pp 46.BACK

8. "Yeltsin Approves List of Security Council Commissions," *Rossiyskaya Gazeta*, 9 Nov 93 p 5. Edict No. 1686 of the Russian Federation President "On Improving the Activity of the Interdepartmental Commissions of the Russian Federation Security Council," dated Moscow, the Kremlin, 20 October 1993 and signed by Russian Federation President B. Yeltsin, followed by "List of Standing Interdepartmental Commissions of the Russian Federation Security Council", which included one on information security.

The U.S. Army protects its information under the provisions of Army Regulation 380-5, Department of the Army Information Security Program. The regulation lays out procedures for classifying, declassifying, marking, disseminating, and safekeeping information, among other subjects. BACK

9. Aleksey Okhskiy, "FAPSI: Only Powerful Organizations are Capable of the Comprehensive Protection of Information," *Sevodnya*, 8 September 1995, p 3 as published in FBIS-SOV-95-188-S, 28 September 1995, p 19.BACK

10. Okhskiy, p 20.BACK

11. Ibid. BACK

12. Sergey Ptichkin, "Top Secret: Unique Technical Developments by FAPSI Specialists," *Rossiyskaya Gazeta*, 8 June 1995, p 8, as reported in FBIS-SOV-95-111, 9 June 1995 p 21.BACK

13. *Izvestiya*, 28 July 1995, p 2, as reported in FBIS-SOV-95-154-S, 10 August 1995, p 24.BACK

14. Ibid.BACK

15. Okhskiy, p 21.BACK

16. S.A. Komov, "O kontseptsii informatsionnoy bezopasnosti strany ("On the Concept of the Country's Information Security") *Voyennaya Mysl* (*Military Thought*), No 4 1994, p 12-13.BACK

17. "National Security in the Information Age," handout received by the author in Moscow in 1995.BACK

18.Sergei Modestov, "Na Nevudimom Frontye-Aktivizatsiya boyevykh deystviy" ("At the Invisible Front-Warfare Activization") *Delovoy Mir* (*Business World*), 24 February, 1994, p 7..BACK

19. Ibid.BACK

20. Aleksandr Pozdnyakov, interviewed by Vladimir Davydov, "Information Security," *Granitsa Rossii*, September 1995, No. 33 PP 6-7, as reported in FBIS-UMA-95-239-s, 13 December 1995, pp 41-44.BACK

21. A. Vladimirov, "Informatsionnoye oruzhiye: Mif ili real'nost'?" ("Information Weapons: Myth or Reality?"), *Krasnaya Zvezda* (*Red Star*) 5 October 1991, p 3.BACK

22. Ibid.BACK

23. R.M. Yusupov and B.P. Pal'chun, "Obespecheniye Bezopasnosti Komp'yuternoi Infosfery," (Safeguarding the Security of the Computer Infosphere) *Vooruzheniye, Politika, Konversiya* (*Armaments, Policy, Conversion*) No. 3 1993, p 23.BACK

24. Yu.V. Lebedev, I.S. Lyutov, and V.A. Nazarenko, "Voyna v zonye Persidskogo zaliva: uroki i vyvody" ("War in the Persian Gulf: Lessons and Conclusions,") *Voyennaya Mysl* (*Military Thought*) No. 11-12, December 1991, p 114.BACK

25. I.N. Vorobyev, "Uroki voyny v zonye Persidskogo zaliva" ("Lessons of the Persian Gulf War,") *Voyennaya Mysl* (*Military Thought*) No. 4-5, 1992, p 69.BACK

26. V. Pirumov, "The Two Sides of Parity and Defense Sufficiency," *Voyennaya Mysl* (*Military Thought*) No. 2 1992, pp 26-34, as reported in JPRS-UMT-92-007-L, 5 June 1992, pp 14-20.BACK

27. Pirumov, p 17. Russians express combat potentials as the combat capabilities of force groupings or of individual systems in the form of a coefficient of commensurability (standard unit of armament, also translated as weapons efficiency index or effectiveness indicator). Information means, according to Pirumov, are expressed "in amounts whose presence and value directly affect the generalized weapon employment effectiveness indicator."BACK

28. In calculating the main components of a force grouping's combat potential (CP_{gr}) Pirumov included the following: - combat potential of weapons (CP_w) (does not include the weapon's information support equipment) - on board autonomous command and control systems and equipment ($DeltaCP_{as}$), intelligence ($DeltaCP_i$), command and control ($DeltaCP_{cc}$), and electronic warfare ($DeltaCP_{ew}$). BACK

29. Ibid.BACK

30. Ibid. Besides Pirumov, other officers foresee a change in military calculations due to precision weapons based on precise information technology. This change has resulted in a

reworked definition of victory. In past wars, victory was defined as: V = A + B + C, where V = victory; A = destruction of opposing military forces; B = destruction of the enemy's economy; and C = elimination of an enemy's political system. These all were accomplished by the occupation of his territory. Future war will have a different definition of victory provided the one side possesses sufficient precision-guided means and weapons based on new physical principles to conduct strikes on a strategic scale. In that case victory is defined as V = A + B where V = victory; A = destruction of enemy means of counter attack, and B = strikes by precision-guided munitions against the armed forces, the economy and national leadership and C3I. The surprise massed use of precision-guided weapons will facilitate the execution of those tasks which earlier were assigned to nuclear weapons, the Russian officers believed. From discussions with Russian officers in Washington in 1994.BACK

31. Ibid.BACK

32.The author would like to thank Dr. Jacob Kipp who spoke with General Belous and shared this information. BACK

33. V. N. Medvedev and S. K. Lopukov, "Problems and Perspectives on the Informatization of the Armed Forces of the Russian Federation," *Equipment. Politics. Conversion*, 1/93, pp 57-60.BACK

34. A. Ya. Vayner, "On Opposition in the Sphere of Command and Control," *Voyennaya Mysl* (*Military Thought*) No. 9, September 1990, pp 18-23 as reported in JPRS-UMT-90-009-L, 21 November 1990, pp 10-13.BACK

35. Yu.V. Lebedev, I.S. Lyutov, and V.A. Nazarenko, p 111.BACK

36. Vayner.BACK

37. Major General Yevgeniy Korotchenko and Colonel Nikolay Plotnikov, "Informatsiya-Tozhe oruzhiye: o chem nel'zya zabyvat' v rabote s lichnym sostavom" ("Information is also a weapon: about what not to forget in working with personnel,") *Krasnaya Zvezda* (*Red Star*), 17 February 1994 p 2.BACK

38. Clifford Reid, "Reflexive Control in Soviet Military Planning," in *Soviet Strategic Deception*, edited by Brian Daily and Patrick Parker, Lexington Books, p 294.BACK

39. Ibid., p 293.BACK

40. M. Ionov, "Control of the Enemy," *Morskoy Sbornik* No 7 July 1995, pp 29-31, as reported in FBIS-UMA-95-172-S, 6 September 1995, pp 24-27.BACK

41. Ibid., p 25.BACK

42. Georgiy Smolyan, Vitaliy Tsygichko, and Dmitriy Chereshkin, "A Weapon That May be More Dangerous Than a Nuclear Weapon: The Realities of Information Warfare," *Nezavisimoye*

Voyennoye Obozreniye (Supplement to *Nezavisimaya Gazeta*), 18 November 1995, no 3, pp 1-2, as translated in FBIS-UMA-95-234-s, 6 December 1995, pp 31-35.BACK

43. Medvedev, p 60.BACK